x509-free access to WLCG resources

Short, H.

2017-11-23

Short , H , Manzi , A , De Notaris , V , Keeble , O , Kiryanov , A , Mikkonen , H , Tedesco , P & Wartel , R 2017 , ' x509-free access to WLCG resources ' , Journal of Physics : Conference Series , vol. 898 , no. 10 , 102001 . https://doi.org/10.1088/1742-6596/898/10/102001

http://hdl.handle.net/10138/298544
https://doi.org/10.1088/1742-6596/898/10/102001

x509-free access to WLCG resources

IOP Conf. Series: Journal of Physics: Conf. Series **898** (2017) 102001 doi:10.1088/1742-6596/898/10/102001

x509-free access to WLCG resources

H Short[1], A Manzi[1], V De Notaris[1], O Keeble[1], A Kiryanov[1 2], H Mikkonen[3], P Tedesco[1] and R Wartel[1]

[1] CERN, Switzerland
[2] B.P. Konstantinov Petersburg Nuclear Physics Institute - PNPI, Russia
[3] Helsinki Institute of Physics, Finland

Abstract.
Access to WLCG resources is authenticated using an x509 and PKI infrastructure. Even though HEP users have always been exposed to certificates directly, the development of modern Web Applications by the LHC experiments calls for simplified authentication processes keeping the underlying software unmodified.
In this work we will show a solution with the goal of providing access to WLCG resources using the user's home organisations credentials, without the need for user-acquired x509 certificates. In particular, we focus on identity providers within eduGAIN, which interconnects research and education organisations worldwide, and enables the trustworthy exchange of identity-related information. eduGAIN has been integrated at CERN in the SSO infrastructure so that users can authenticate without the need of a CERN account.
This solution achieves x509-free access to Grid resources with the help of two services: STS and an online CA. The STS (Security Token Service) allows credential translation from the SAML2 format used by Identity Federations to the VOMS-enabled x509 used by most of the Grid. The IOTA CA (Identifier-Only Trust Assurance Certification Authority) is responsible for the automatic issuing of short-lived x509 certificates. The IOTA CA deployed at CERN has been accepted by EUGridPMA as the CERN LCG IOTA CA, included in the IGTF trust anchor distribution and installed by the sites in WLCG. We will also describe the first pilot projects which are integrating the solution.

1. Authentication for Distributed Virtual Organisations

In High Energy Physics (HEP), research groups are typically highly distributed over institutions and geographies. It cannot be assumed that all team members are able to register with a central identity provider and, consequently, remote credential provisioning and identity vetting is required. Although this challenge is not new, recent developments in Federated Identity Management (FIM) present interesting opportunities for improving online security and user experience for collaborating researchers.

1.1. Certificate Authentication and its Disadvantages

At The Worldwide LHC Computing Grid (WLCG), authentication is currently provided via x509 certificates, issued by Interoperable Global Trust Federation (IGTF)[5] accredited certificate authorities. An individual user is able to obtain a certificate from a registered certificate authority and, through a local registration authority, prove their identity. This personal certificate represents the researcher's identity online and can be registered with their virtual organisation's membership management tool. In the case of the WLCG, this tool is VOMS[11], the Virtual

Organisation Membership Service.

x509 certificates are an essential component of internet security and are well suited to machine-to-machine communication. However, certificates should not be owned and managed by end users for a number of reasons, some of which are discussed here. Firstly, coupling credentials with devices (or even browsers) creates a burden on users whenever a service must be accessed via a new channel. The certificate must be installed in the target browser and should subsequently be removed if the device is not owned by said user. Certificate management is not in the skillset of the average early career researcher. With poor understanding of certificates comes an increased security risk of individuals leaking public keys, or leaving certificates installed on shared devices. Users are accustomed to simpler access methods, username and password, and are expecting single-sign-on as provided by multiple, large public identity providers. If research and education is unable to match the smooth user experience provided by such identity providers, the community risks users resorting to using identities outside of our control for research activity.

1.2. Federated Identity Management

Federated Identity Management (FIM) has become a key enabler for international collaboration within research and education. The ability to use one's home organisational account to access shared services streamlines account maintenance at participating entities and provides a unified experience for end users. Over the past five years, FIM has established itself as a standard service offered by thousands of universities and research organisations; over 60 national federations are operational, with more set to follow[7].

A federation can be described succinctly as a group of service providers and identity providers that agree to interoperate under a shared policy set, such that a user from a participating identity provider is able to access any participating service. Federations tend to be geographically bound with policies reflecting the national law and funding structures. To truly enable global research and collaboration, FIM has been extended internationally via eduGAIN, the inter-federation service[9], which links these national federations.

2. HEP Requirements for FIM

Can eduGAIN be used out-of-the-box by the High Energy Physics community? We, the authors, believe not and that several factors must be addressed before wide-scale adoption of FIM for HEP can take place.

2.1. Trustworthy Users

The inter-federation service eduGAIN contains over 2000 Identity Providers[9] as of October 2016. In the original SAML2.0 specification there was no indication of these participants' security capability or willingness to collaborate in incident response. Effective incident response for federations is one of the requirements identified in the 2012 FIM4R paper[1] that identified the needs of multiple research communities. The Security Incident Response Trust Framework for Federated Identity, or Sirtfi[8], is a means to identify those identity providers able and willing to participate in incident response. An active security contact must be provided by these entities, forming the first point of contact in an incident. Sirtfi can be used by the HEP community to identify which of the 2000 Identity Providers they can trust to a higher degree.

A similar scheme for identifying the subset of eduGAIN to work with is the REFEDS[7] Research and Scholarship entity category. This framework can be used to identify which Identity Providers serve the research and scholarship community and release the core set of attributes (name, email and identifier) required by most research service providers.

By using both Sirtfi and the Research and Scholarship entity category, the HEP community can identify which eduGAIN Identity Providers to interact with. In addition to identifying the Identity Providers, HEP can make use of its existing databases of Virtual Organisation membership to ensure that only known users are given access to critical resources.

2.2. Command-Line Access

The SAML2.0 protocol's primary use case is web based authentication but the bulk of the HEP users' workflow is performed on the command line. Although there is an alternative protocol for command line access, the Enhanced Client or Proxy (ECP) protocol, very few Identity Providers have enabled this authentication method. Other methods depend on interaction with a web browser, which may be inconvenient or even impossible in certain use cases.

To provide a workaround for command-line access, a prototype service called educert[22] has been developed at CERN. This web service transforms SAML tokens directly into grid proxy certificates for download. There are various pilots ongoing through the AARC project to provide scalable and sustainable access to research infrastructures using FIM[4]. Fundamentally, all solutions require a token translation service to convert from SAML2 to the target token, primarily x509.

2.3. VOMS authorization

VO membership is controlled via VOMS, which governs the identities, roles and groups within a VO. Maintaining user management and authorization with VOMS is essential for a smooth integration of FIM with existing HEP technologies. Currently, VOMS defines users based on their personal x509 certificates. The challenge here is twofold: to allow VOMS registration with SAML2 credentials and to associate x509 credentials from existing VOMS records with their SAML2 counterparts.

Linking the x509 and SAML2 credentials owned by an individual is non-trivial, generally there is no single field shared between the two. A dual authentication process should be implemented in order for users to associate their various credentials. At CERN for instance, VOMS registration requires validation of an email address that is already linked to a CERN account and has been vetted by CERN HR. A key benefit of FIM is the reduced need to create local accounts, i.e. CERN accounts in this context. Once local accounts are no longer created, how will identity vetting be performed and will it be possible to associate a VOMS registration request with a known, vetted user?

There are many unanswered questions regarding VO membership and authorization in the FIM environment. This will be discussed in more detail in the Security Whitepaper being produced in the HEP Software Foundation[12].

3. Technical Implementation

In order to remove certificate management from the hands of the users, whilst maintaining access control to WLCG resources with x509 certificates, a token-translation middle layer is required. To satisfy the identified requirements for the adoption of Federated Identity Management by the HEP community, the token translation from SAML2.0 to x509 should be governed by VOMS authorization and result in an x509 certificate with an appropriate lifetime. We, the authors, propose the following solution to provide transparent access to WLCG Web Services. The key components are discussed in further detail below. A full guide to implementation can be found on CERN's Authentication Portal[10].

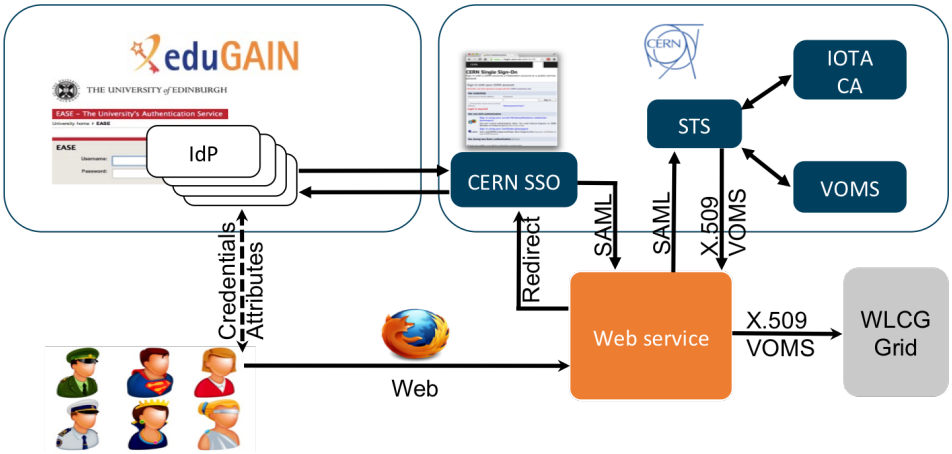

Figure 1. Components required for transparent access to x509 controlled resources for eduGAIN users.

3.1. CERN Single-Sign-On

The CERN Single Sign On (SSO) service provides a central authentication mechanism for all CERN applications.
The service, which is part of the eduGAIN federation and the Sirtfi framework, allows users to authenticate with credentials issued by CERN or any Sirtfi-compliant eduGAIN Identity Provider. Application owners can restrict access to their application to CERN users or federated users, and configure multi-factor authentication requirements.
Each Web server that is integrated with CERN SSO must be properly registered and needs one extra component: an SSO plug-in, which handles interaction with SSO and provides standard authorization hooks to the Web server. For Apache on Linux there are two possible solutions both supported at CERN:

- Shibboleth[15] : widespread, supports all possible standards and can also be used as SSO server software. This is the first solution that was supported at CERN. The only shortcoming of Shibboleth is a complex XML-based configuration.
- Mellon[16] : lightweight and pure SAML2 Service Provider with simple configuration.

Through these plugins a user's SAML Assertion can be exported from the CERN SSO Service and sent to STS for transformation into an x509 certificate.

3.2. Security Token Service

The Security Token Service (STS)[13] takes SAML tokens, or username and password pairs, and transforms them into x509 certificates. The original STS implementation was performed in the context of the EMI3 project and recently it has been extended to:

- Use a IOTA CA to generate short-lived certificates
- Integrate VOMS in order to generate a certificate only for members of a Virtual Organisation and perform the association with the generated IOTA CA certificate Distinguished Name

Lastly, in order to streamline the deployment of the STS service for new VOs and services, we have also developed a Puppet module[14] which is integrated in the CERN Puppet infrastructure.

3.3. CERN LCG IOTA Certificate Authority

The CERN LCG IOTA Certification Authority[17] issues certificates through a set of Security Token Services.
Each STS accepts requests from a single client application, and is restricted to issue certificates only for a set of allowed VOs. To use the CERN LCG IOTA CA, a user must be authenticated by an Identity Provider belonging to the eduGAIN federation and capable of providing a unique and persistent user identifier (typically through the "eduPersonPrincipalName" attribute). The user must also be fully registered in the VOMS service as members of one of the LHC VOs.
Client applications authenticate to the STS with the user's federated credentials, and request the creation of an STS certificate for the user in the context a virtual organization. The certificate request must contain the user's SAML authentication token (which must include a federation-wide unique and persistent identifier for the user), and the name of a Virtual Organisation to which the user belongs, and for which the STS service instance is allowed to release certificates. The Security Token Service will then verify the correctness of the received data, and, if necessary, request a certificate for the user to the Certification Authority. User certificate obtained from the CA have a lifetime of one week, and can be cached by the STS service to be reused for future requests. The user certificate released by the CA is in turn used to sign a proxy certificate for the user, containing the VOMS extensions for the user. Finally, the proxy certificate is returned to the client application from the STS service.
In order to allow the usage in the WLCG context the CERN LCG IOTA CA has been reviewed and accepted by EUGridPMA and distributed as part of the IGTF Trust Anchors Distribution[6] and the usage in WLCG has been also discussed and approved by the WLCG Management Board[18]

3.4. VOMS

The Virtual Organisation (VO) Membership Service (VOMS) governs Authorization for WLCG services. A user is assigned roles and groups and is able to generate proxy certificates permitting short term access to resources requiring proof of membership. At the moment VOMS registration is limited to users with a personal x509 certificates, therefore STS assumes that the users accessing via eduGAIN and members of a VO have already a personal certificate. This limitation is going to be removed in future versions of VOMS, which will allow registration of users without the need of an x509 certificate.
In the current implementation, the STS service is deployed and configured to have administrative VOMS access in order to:

- List the users members of a VO
- Associate (if not yet present) the IOTA CA certificate DN to the existing user DN

3.5. Kipper

Kipper[19] is a collection of client side software and configuration which enables the exploitation of the solution service described in this paper. It has been developed in order to ease as much as possible x509 manipulation and hide the interaction with the STS service. The software includes JavaScript, PHP and Python snippets/functions which are already used in the available deployments described in the next section.

3.6. Deployments

The solution presented here has been enabled for a pilot with WebFTS[20] (Web file-transfer service) which transparently delegates IOTA CA proxies to the back-end to perform file transfers. The ATLAS collaboration has already enabled CERN Single-Sign-On for their Job monitoring service (BigPanda[21]) and will use the pilot to provide user level access control to job logs.

Educert[22], the prototype service offering VOMS Proxy Certificate downloads, is based on this solution and provides a workaround for command-line access.

4. Conclusion

Federated Identity Management and eduGAIN offer the WLCG Community an interesting opportunity to modernise remote user authentication and remove certificate management from the hands of the researchers. However, there are three main topics that should be addressed before widespread adoption; identifying trustworthy participants, enabling access to non-Web services and integrating FIM into VOMS processes.

The x509-free service required for transparent access to Web Services for eduGain users is available for VOs and a guide has been developed[10]. The current system offers authentication for existing VOMS users, identified by a VOMS attribute. Although this solution is attractive for web-based services, additional work is needed to create a viable command line access mechanism with no reliance on web interaction.

References

[1] "Federated Identity Management for Research Collaborations", Broeder D et al, April 23 2012, CERN-OPEN-2012-006,
https://cdsweb.cern.ch/record/1442597
[2] "Raising Security and Trust in our Inter-Federated World", Short H et al, in the Proceedings of the International Symposium of Grids and Clouds 2016 (ISGC 2016), Taipei, Taiwan, March 13-18, 2016, PoS (ISGC 2016) 030
[3] "A Trust Framework for Security Collaboration among Infrastructures", Kelsey D et al, in the Proceedings of the International Symposium of Grids and Clouds 2013 (ISGC 2013), Taipei, Taiwan, March 17-22, 2013, PoS (ISGC 2013) 011
[4] AARC, Authentication and Authorization for Research and Collaboration,
https://www.aarc-project.eu
[5] Interoperable Global Trust Federation,
https://www.igtf.net
[6] IGTF Trust Anchors Distribution,
https://dist.eugridpma.info/distribution/igtf/
[7] REFEDS, the Research and Education Federations Group,
https://www.refeds.org
[8] A Security Incident Response Trust Framework for Federated Identity v.1,
https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
[9] eduGAIN,
https://www.edugain.org
[10] Implementation guide, WLCG Federated Access,
https://espace.cern.ch/authentication/CERN%20Authentication/WLCG%20Federated%20Access.aspx
[11] Virtual Organisation Membership Service, VOMS,
http://italiangrid.github.io/voms/index.html
[12] HEP Software Foundation,
http://hepsoftwarefoundation.org
[13] Security Token Service,
https://twiki.cern.ch/twiki/bin/view/EMI/EMISTSDocumentation
[14] Security Token Service puppet module,
https://gitlab.cern.ch/ai/it-puppet-module-sts
[15] Shibboleth,
https://shibboleth.net/
[16] Mellon,
https://github.com/UNINETT/mod_auth_mellon
[17] CERN LCG IOTA CA,
https://cafiles.cern.ch/cafiles/certificates/list.aspx?ca=iota
[18] CERN LCG IOTA CA WLCG MB approval,
http://www.nikhef.nl/grid/tmp/WLCG-CERN-IOTA-statement-MB-20151028.pdf

[19] "Kipper a Grid bridge to Identity Federation", Kiryanov A et al, in the Proceedings of the International Symposium of Grids and Clouds 2016 (ISGC 2016), Taipei, Taiwan, March 13-18, 2016, PoS (ISGC 2016) 017
[20] Webfts Portal,
`https://webfts.cern.ch`
[21] BigPanda Portal,
`https://bigpanda.cern.ch`
[22] Educert Portal,
`https://educert.cern.ch/`